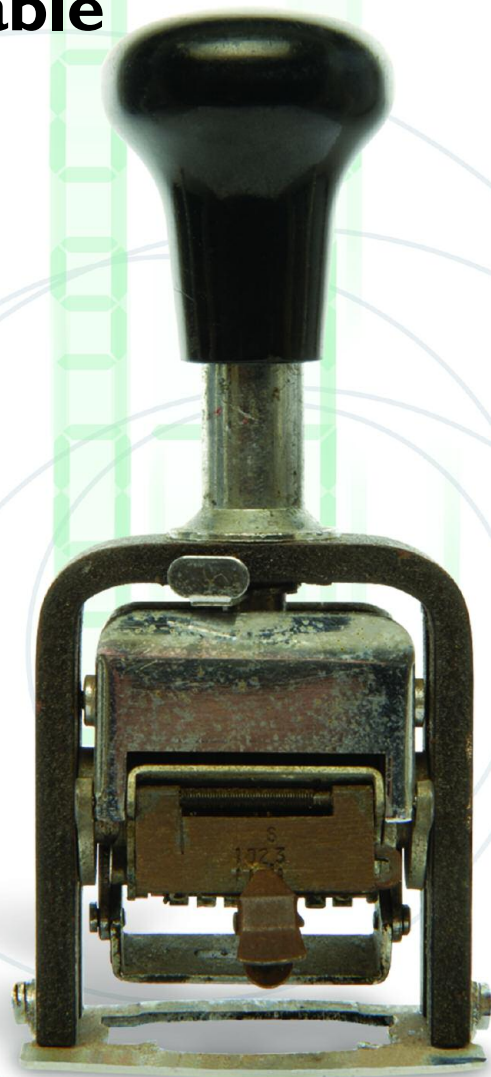


# **Integrated Watermarking Creates More Durable Pay-TV Businesses**



## Integrated Watermarking Creates More Durable Pay-TV Businesses

Managing and monetizing digital content throughout its lifecycle is becoming more complex for network operators and content owners alike. Pressure for innovative business approaches are driven by ever more demanding consumers and the growing capacity of broadband connections. Furthermore, new media outlets and video-enabled devices are up-ending established business models.

Of course, content piracy continues to be recognized as a challenge to the fundamental business processes of the industry. However, this environment presents as many new opportunities as it does threats. Content owners are examining if more transparent and inclusive distribution policies will maximize profits through broader consumption or risk eroding profits through piracy.

This whitepaper will focus on how digital video watermarking can directly address some key challenges in the revenue protection and generation picture of content distribution systems. In particular, it will illustrate how watermarking technologies can be effective in deterring piracy, opening up new business models and reducing the challenges of content portability. As an integrated part of a layered distribution model, the true potential of this technology can be vividly demonstrated.

### Competing with Free

There are many dimensions of the illegitimate video distribution world. From the two-edged sword of YouTube's meteoric rise in popularity, where online video clips can seemingly attract a larger audience than the initial broadcast, to the politics of peer-to-peer (P2P) file sharing, to the lucrative business of mass producing knock-off DVDs. It is easy to underestimate the potential business impact of a highly anticipated movie that becomes freely available through a rogue channel even before the initial theatrical release.

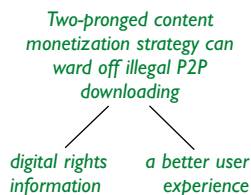
It seems that competing with "free" is now an accepted fact of life in the content and distribution industries and many consumers seem undeterred by arguments about

depriving content owners of their legitimate revenue streams. In an LA Times /Bloomberg survey of young people aged 12-17, 58% believed it was okay to copy a DVD from a friend.<sup>1</sup>

This attitude however, seems open to influence. In another major survey conducted by Interpret, LLC, on behalf of the Digital Watermarking Alliance, consumers identified that ease of access was a major factor in their reasons for illegally copying content.<sup>2</sup> The survey also found their sharing and copying might be dramatically reduced – by up to 50% – if the copyright restrictions were reinforced through some system of traceable marks, particularly if such marks did not enforce any physical digital rights management (DRM)-like restrictions on use of the files.

In a system where the value of movie content is tightly bound to a series of calibrated release windows, legitimate early release distribution presents big opportunities for network operators. Modifying release window policies also presents new challenges for protecting and extending that revenue stream.

According to Keith Nissen, In-Stat analyst, “The question is whether the video industry wishes to control its own destiny, or get crushed by technological change, similar to what is occurring in the music business.”



In a recent report, In-Stat endorsed the shift in the video industry’s approach of digital rights management towards content monetization.<sup>3</sup> A migration of P2P power user households to legal video services would generate \$1.4 billion in subscription revenue and \$1.1 billion in advertising revenue annually. In-Stat’s report advocates a two-pronged content monetization strategy using all the various DRM tools available and offering a better user experienced compared to illegal P2P downloading.

The story of the notorious file sharing site Pirate Bay certainly illustrates this shift. After Pirate Bay’s co-founders were convicted of collaborating to violate copyright law, Swedish company Global Gaming Factory X AB offered to buy the company for nearly \$8 million. The site’s potential owners have indicated their intention “to launch new business models that allow compensation to content providers and copyright

<sup>1</sup> LA Times, *Is Copying a Crime? Well...*, Aug. 9, 2006.

<sup>2</sup> Digital Watermarking Alliance and Interpret, LLC, *Consumer Strategies for Deterring Illegal File-Sharing Using Digital Serial Numbers*, May 28, 2009.

<sup>3</sup>In-Stat, *Adopting Digital Rights Information Management*, Jul. 7, 2009.

owners.” However it remains to be seen if Global Gaming Factory can successfully capitalize on the brand of a site associated with “free.”

It is clearly up to the studios and pay-TV operators to maintain consumer motivation to actually pay-per-view by emphasizing and reinforcing the value add of legitimate content over “free” illegitimate downloads. An effective extra layer to the revenue protection regime can make the difference between a few subscribers that distribute movies to a large Internet community and a growing consumer base that values legally acquired content.

### Layered Protection Techniques

Protection technologies that underpin the content business process fall into two broad categories. The first is encrypted delivery techniques, where key management distinguishes between those that have acquired rights to consume digital content and those do not have such rights. The second category of techniques is those that help track and monetize any copies that are reproduced, such as watermarking and fingerprinting.

For this second category, there are generally two approaches:

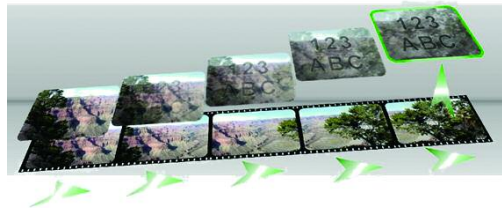
- 1) To enable the tracing of an illegal copy to the last authorized recipient based on display location, time or device information. The presence of a **forensic mark** acts as a deterrent once the consumer is made aware – beforehand – that the content is traceable to the last authorized recipient. It also allows action to be taken in subsequent investigations and removes the infringer’s perceived safety of anonymity.
- 2) To help **recognize and identify the content** in illegitimate distribution channels. This allows monitoring distribution and playback channels to control and enforce content distribution rules.

The Digital Watermarking Alliance, an international alliance of industry leading organizations that deliver valuable digital watermarking solutions, offers several papers evaluating these complementary techniques on its website, [www.digitalwatermarkingalliance.org](http://www.digitalwatermarkingalliance.org)

Despite multiple research efforts, no single technology currently exists that can defeat or prevent all types of threat. For instance, with today's high definition (HD) displays and advanced camcorders, it is possible to circumvent some of the layers of protection technology with a high-quality recording of content that is playing on a flat screen television.

Yet each protection technique that is deployed tends to chip away further at any potential commercial reward for pirates. Increasing the effort required to mount an attack on any source of content will delay piracy and allow crucial time for revenue generation. Furthermore, content degradation (e.g. via camcording) will decrease the quality of pirated content and hence the value of resulting copies.

*Layered protection solutions can delay piracy and allow time for revenue generation*



Increasingly sophisticated content and revenue protection solutions employ layers of these techniques to address the different types of threats that occur in various markets. For example, many advanced pay-TV systems can combine applications of encryption, output protection, on-screen fingerprinting and watermarking mechanisms to address the challenges of illegal distribution for certain types of high value material.

### **Versatility of Watermarking throughout Value Chain**

According to MultiMedia Intelligence, applications leveraging content identification technologies, such as digital watermarking and fingerprinting, are growing rapidly and could surpass \$500 million worldwide by 2012.<sup>4</sup> The research firm identified several key applications for these technologies, including Internet and broadcast content monitoring, metadata association, copyright control, content protection and forensics and interactive advertising.

The firm's report highlighted that watermarking can be used for different purposes at various stages during the content distribution cycle: in the studio, in the distribution

<sup>4</sup>MultiMedia Research, *Beyond Traditional DRM: Moving to Digital Watermarking & Fingerprinting in Media Monetization*, Jan. 21, 2008.

network, and in the receiver. Moreover, multiple watermarks from different sources can in principle be applied to the same content and extracted individually later. Forensic tracking is thus enabled at multiple stages in the value chain, with the possibility to trace any lost content within the chain, including its last authorized user.

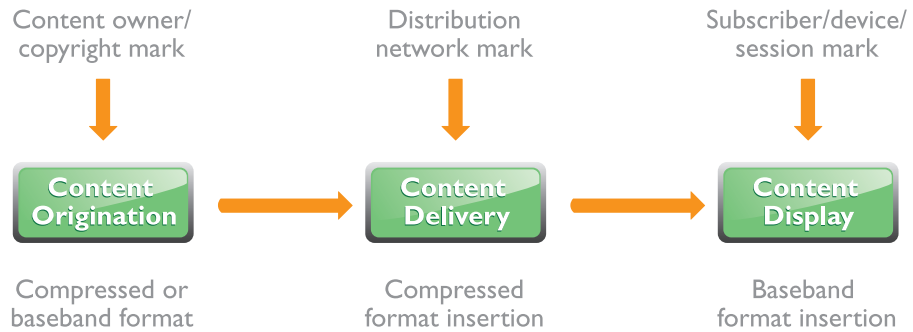


Figure 1: Watermarking Insertion Points

One key division of techniques highlighted by this multi-step workflow is the use of compressed domain watermark insertion versus baseband insertion. Insertion of watermarking images in baseband video can only occur at very discrete points in today’s distribution networks, each with its own limitations. For instance, the modification of media content after decompression in the client device (e.g. set-top box) must be implemented in a processing environment that offers a relatively small amount of processing power. It becomes important to use an efficient watermarking system that can modify video frames with low latency and high efficiency.

The modification of compressed content in locations that do not decode or re-encode content, such as content aggregators, is also a particular challenge. New generations of compression formats, such as H.264, are highly efficient and leave little remaining redundancy that can be used for image modification. Small variations of the compressed bitstream may have a significant and potentially uncontrollable effect on the decompressed video output. Algorithms are required that take the specifics of the compression format into account and apply surgical modification to predetermined locations that result in a robust mark in serialized streams without content re-encoding or storage of multiple content files.

<sup>4</sup> CNet, “Echostar, WebTV team on TV service,” Apr. 26, 1999.

<sup>5</sup> Sky, “Sky Launches Sky Player TV - New Online Only Subscription TV Service,” Dec. 4, 2008.

The following examples describe how watermarking adds value at different stages of the media lifecycle and in different parts of the content distribution channel.

- **The Digital Studio** – Dailies and early edited copies of content are especially valuable and potentially vulnerable. As studios transition to increasingly digital production processes, there is a proliferation of high-quality digital copies of this material created on networks and on transportable media. Watermarking each copy of content that is distributed permits today's studios to accurately identify sources of unauthorized copies and identify business partners that leak content and need to improve their workflow security.
- **Theatrical Distribution** – First run movies are attractive targets for content pirates. As well as the vulnerability of very high-quality media used for movie projection, there are also individuals attempting to use camcorder equipment to capture a live copy of the presentation. These captures are the source for many pirate distributions on DVD. Watermarking is used in digital cinemas to insert location and date/time information to the projected image that allows identification of theaters and screenings that are a common source of piracy.
- **Content Distribution Network** – Since watermarks are invisible in normal viewing conditions, it is often possible to add successive marks as the digital content moves through the distribution channel. For instance, one type of watermark is added as the content files are provided to aggregators or system operators. Another specific watermark is added as content is ingested to a video-on-demand (VOD) system. If unauthorized copies of content are found and analyzed, from the number of marks found and the data contained within them, it becomes possible to identify at which point in the distribution chain the copy was made. In addition, cases of local re-broadcasting of content from satellite systems can be traced back to the legitimate rights owner.
- **Hospitality** – With access to a growing array of pay-per-view (PPV) content released in the hospitality window, e.g. pre-DVD and often in HD format, hotels have become targets for content pirates. By direct capture or via camcorder, in the privacy of a

room, pirates can attempt to make higher quality copies of movies and other material. Again, watermarking provides a valuable tool to trace and curtail these kinds of activities by marking any copies with timestamps and location detail of the property and room to identify the perpetrators.

- **Consumers** – While home recording of movies for personal use is permitted, the potential exists for significant commercial loss through large scale distribution over the Internet. Watermarking, especially conspicuously flagged watermarked material, helps to change the perspective of individual liability for misuse of any copies made. When an individual realizes that a movie is a personalized, registered copy there is considerably more incentive to prevent misuse.
- **Mobile and Low Bit rate Distribution** – One issue that bedevils the media industry is ensuring transparency of consumption for consumers. As noted above, sharing of media files across devices is more or less an everyday experience. The challenge for a network operator in supporting DRM file formats and matching back-end system for all devices their subscriber may want to legitimately use could be daunting. With access to a powerful watermarking technology, this burden can potentially be reduced for mobile devices by offering portable clear copies of content that carry an identifying source watermark. This approach trades off the piracy issues around copying of low bit rate content against the value the consumer puts on ease of use. Any commercial level of illegitimate copying at least can be traced back to the source as with the examples above.

### Following the Money – Forensic Watermarking

One of the most promising techniques to track unauthorized copies is user-specific forensic watermarking, which seeks to securely, robustly and imperceptibly hide information within media content. Unlike encryption, which creates an envelope around content that can effectively secure delivery from point to point, a watermark takes the form of a digital serial number (DSN) that is embedded in the content itself and remains there even if the content has been decrypted, decoded and possibly re-recorded and re-encoded to a different file format.

Each aspect of forensic watermarking emphasized above benefits from a little amplification:

- **Imperceptible marking** is required to preserve the important quality of the viewer experience and to avoid any implication that the delivery channel using watermarking reduces the integrity of the original material. The use of imperceptible marking draws a specific contrast to some visible video overlay techniques used to help trace illegitimate channel rebroadcasting.
- **Security** is necessary to preserve the integrity of the inserted information, and especially to prevent any modification of embedded watermark information as copies are distributed. If an embedded DSN could easily be altered in place, tracking mechanisms might give fatally incorrect results. If the DSN integrity is unquestionable, then the information on origination of the material can be useful for copyright enforcement actions.
- **Robustness** ensures that the watermark remains readable through any reasonable manipulation or transformation of the media. The most robust watermarks will survive multiple transitions from digital to analog format and back. The approach of re-recording from an analog output of a playback device, circumventing all encryption and other control mechanisms, is sometimes termed the “analog hole” through which content can escape. Robust watermarking techniques will embed a DSN that can survive the passage through the analog hole, enabling identification of unauthorized copies that are produced using, for example, a camcorder that is placed in front of a TV.

In comparison to other digital media such as audio, digitally distributed movies can be protected particularly well by forensic watermarking. Digital video is a composition of many individual images and corresponding audio information, with a much larger amount of data than any other common media file and with more scope to robustly embed information. With advanced methods that make use of the density of information to insert watermarking payloads, video watermarks can be vastly more effective in all the respects identified than audio or textual information. The latest commercial watermarking technologies are robust against attempts of removal, such as re-encoding or even targeted filtering attacks.

Forensic watermarking takes on a special value when the embedded DSN is employed to help identify the source of unauthorized copies and trace them back to the last authorized recipient or the rightful content owner. The mark used in this way does not enforce content use restrictions, but it allows identification of sources of content abuse, acting as a deterrent and encouraging responsible consumer behavior. It is a way to maintain control over the content while enabling more convenient content use that can compete with free, which is typically of lower quality and illegally distributed.

### Forensic Tracing at Work

A user-specific solution is designed to identify the exact delivery of a video copy. Much like a license plate for a car, the video contains a device identifier that can be traced to the individual consumer of a video copy. In addition



to static information, the mark contains a time stamp that relates to a playback time and date. The complete process is outlined below as an example of video delivery to a subscriber set-top box (STB).

In this scenario in Figure 2, a compressed and encrypted video (0) is delivered to a subscriber's STB (1). The STB, enabled with the watermarking solution, embeds invisible ID information in this content before it leaves the STB. The information can identify the receiving STB, time and operator of the authorized content. This mark does not affect fair and legal consumer use of the content and is transparent during normal display and personal-use recording (2). However, if the content is illegally distributed, e.g. on a DVD or through P2P networks over the Internet (3), the video can be identified either through targeted analysis of a distributed copy or by a piracy watch service that monitors publicly available video content (4). From these copies, the embedded user identification can be extracted (5) even after video quality is degraded by heavy compression or other alterations. The user ID information contained in the distributed copy pinpoints an individual illegally distributing the content (6) and can be used to hold them accountable by either denying future service or by initiation of a criminal investigation.

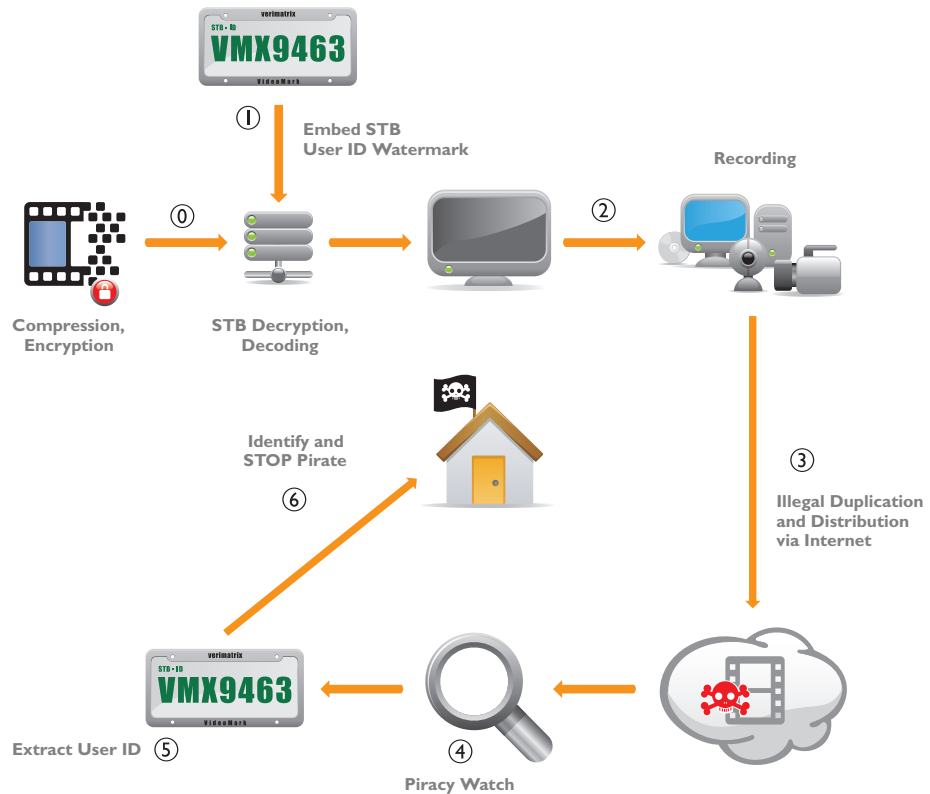


Figure 2: User-specific forensic watermarking can identify the last authorized recipient of content based on set-top ID and time stamp

### Conclusion

With the diversity of challenges and opportunities in the digital video business environment, innovation in revenue security becomes of paramount importance. Watermarking technology offers a mature and robust set of solutions to a variety of thorny consumer and commercial areas. While the initial thrust of watermarking proponents was to advocate its deployment as a legal tool in the fight to deter content piracy, the newer perspective of its use promotes a broader and more positive impact on digital video businesses.

Stand-alone watermarking solutions at different points in the distribution channel of video fill a variety of needs in the growing business of digital video distribution. But the real advantages of this technology are realized when watermarking is integrated into a layered security solution, which in turn helps build more durable pay-TV businesses for now and the future.

Multi-layered content protection strategies have the power to stratify the value of content based on quality, timing and the consumption device for innovative business models. Demonstrating robust protection techniques will enable some operators to obtain higher value material – such as early release HD movies. Watermarking is also a tool with the potential to protect and grow the competitive advantage and market of pay-per-view and over-the-top (OTT) video. Moreover, these layered security techniques are proving to play a special role that is commercially effective and culturally acceptable.